

EXHIBIT 34

(<https://attendee.gotowebinar.com/register/5394704745072711695?source=ammedia>)



7 апреля выходит новое российское ПО класса DCAP. Орлан — ИБ с русской душой. Зарегистрироваться >>

(<https://orlansec.ru/>)

[Главная \(/\)](#) » [Новости \(/news\)](#)



Новый уровень DevSecOps

7 апреля на онлайн-митапе эксперты Positive Technologies расскажут, как выйти на новый уровень безопасной разработки с помощью PT Application Inspector 4.0.

(https://promo.ptsecurity.com/application-inspector?utm_source=antimalware&utm_medium=banner-200-160&utm_campaign=ai4)

Подробнее » (https://promo.ptsecurity.com/application-inspector?utm_source=antimalware&utm_medium=banner-200-160&utm_campaign=ai4)

Google обвинила двух россиян в создании мощного ботнета Glupteba

Екатерина Быстрова (/Users/Ekaterina-Bystrova) 08 декабря 2021 - 09:17

[Корпорации \(/corporate_security\)](#)

[Государство \(/state_security\)](#)

[Windows \(/os/windows\)](#)

[Google \(/companies/google\)](#)

[Ботнет \(/threats/botnet\)](#)



Google (/companies/google) обвиняет двух граждан России в организации сложной кибероперации и создании ботнета. По словам американского интернет-гиганта, обвиняемые заразили более миллиона Windows-устройств по всему миру.

Дмитрий Старовиков и Александр Филиппов — именно эти имена фигурируют в обращении Google. Корпорация утверждает, что граждане России стояли за атаками ботнета Glupteba. Также упоминается множество аккаунтов Gmail и Google Workspace, которые помогали Филиппову и Старовикову в проведении кибератак.

Сеть ботов, согласно заявлению Google, использовалась в криминальных целях: для кражи и несанкционированного доступа к учётным данным пользователей Google-аккаунтов. С 2020 года

злоумышленникам удалось заразить более миллиона компьютеров, работающих на Windows.

Киберкампания Glupteba набрала обороты до такого масштаба, что каждый день атакующим удавалось пополнить ряды ботов тысячами новых устройств. Как правило, заражать устройства преступникам удавалось с помощью вредоносных сайтов, заманивая на них жертв. Обычно такие ресурсы предлагали бесплатно скачать какой-либо софт.

«В любой момент вся мощь ботнета Glupteba могла быть направлена на организацию мощной DDoS-атаки. Стоит также отметить, что Glupteba отличается от других ботнетов сложной технической реализацией — например, использованием блокчейн-технологии», — пишем (https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/1_Complaint.pdf) (PDF) Google в своём обращении в Федеральный окружной суд Южного округа Нью-Йорка.

По данным американской корпорации, операторы Glupteba атаковали цели в США, Индии, Бразилии, Вьетнаме и Юго-Восточной Азии.

СЛЕДУЮЩАЯ ГЛАВНАЯ НОВОСТЬ »



(<https://zen.yandex.ru/id/5a95363da936f43fa2d8ea19>)

Подписывайтесь на канал "Anti-Malware" (<https://zen.yandex.ru/id/5a95363da936f43fa2d8ea19>) в Яндекс Дзен, чтобы первыми узнавать о новостях и наших эксклюзивных материалах по информационной безопасности.

Читайте также

На фоне санкций Информзащита запустила услугу экспресс-аудита рисков ИБ (/news/2022-03-21-111332/38372)

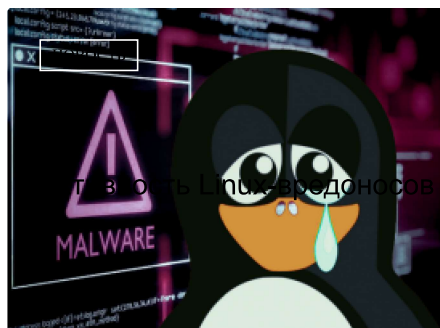
ФСТЭК России приостановила действие 56 сертификатов (Microsoft, Cisco, др.) (/news/2022-03-24-111332/38397)

Уязвимости в Dell BIOS актуальны для миллионов XPS, Inspiron, Vostro (/news/2022-03-22-114534/38382)



Kaspersky сообщила о рекордном числе DDoS-атак за всю истори... (/news/2022-02-22-111332/38223)

(/news/2022-02-22-111332/38223)

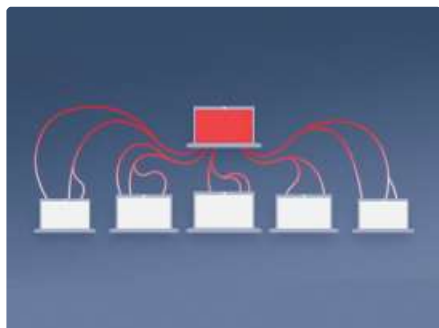


Популярность Linux-вредоносов выросла на 35% в 2021 году (/news/2022-01-17-1447/37970)

(/news/2022-01-17-1447/37970)

НОВОСТЬ

Windows-машины атакует Kraken — новый Golang-бот в стадии ра... (/news/2022-02-17-114534/38199)



(/news/2022-02-17-114534/38199)



Обзор защищённых платформ и накладных средств безопасности больших данных
(/analytics/Market_Analysis/Big-Data-Protection)

(/analytics/Market_Analysis/Big-Data-Protection)



Как удобно и выгодно применять биометрическую аутентификацию в корпоративной среде
(/analytics/Technology_Analysis/Corporate-Biometric-Authentication)

(/analytics/Technology_Analysis/Corporate-Biometric-Authentication)

Система анализа софта CodeScoring добавлена в реестр российского ПО (/news/2022-03-25-111332/38409)

Екатерина Быстрова (/Users/Ekaterina-Bystrova) 25 марта 2022 - 20:10

Малый и средний бизнес (/smb_security) Корпорации (/corporate_security)

Системы для анализа защищенности информационных систем (/security/security-check)

Аудит информационной безопасности (/security/Information-Security-Audit) Сканеры исходного кода (/security/source-code-analysis)

Система композиционного анализа программного обеспечения
CodeScoring официально добавлено в реестр российского ПО.
Официальный дистрибьютор продукта в России — компания Web
Control.



(/news/2022-03-25-111332/38409)

Современная разработка ИТ-продуктов активно применяет программные компоненты с открытым исходным кодом (OSS, Open Source Software). Практически всегда таких компонентов на порядок больше, чем проприетарных.

Использование OSS даёт значимое ускорение разработки, но при этом его бесконтрольное использование увеличивает риски для безопасности. Для управления этими рисками применяются решения класса композиционного анализа ПО (SCA, Software Composition Analysis), которые автоматически определяют используемые OSS зависимости, показывают найденные в них уязвимости и предоставляют информацию об их устранении.

Продукт CodeScoring (<https://codescoring.ru/>) может повысить безопасность использования Open Source на всех этапах обеспечения жизненного цикла разработки программного обеспечения. База знаний CodeScoring содержит собираемый из крупнейших репозиториях

реестр компонентов, который регулярно обогащается данными об имеющихся в них уязвимостях и лицензиях, получаемых из различных источников. CodeScoring поддерживает ключевые OSS экосистемы популярных языков программирования, такие как Maven, PyPi, NPM, RubyGems и др.

CodeScoring содержит следующие функциональные возможности:

Автообнаружение зависимостей — анализ состава кода, автоматическое нахождение файлов манифестов пакетных менеджеров, выявление прямых и транзитивных зависимостей открытого программного обеспечения (OSS).

Ведение реестра компонентов программных проектов (SBOM).

Проверка совместимости Open Source лицензий — выявление лицензий для обнаруженных OSS зависимостей и проверка их совместимости между собой на основании интегрированных политик.

Выявление уязвимых Open Source компонентов в программных проектах на основании актуальной информации из авторитетных источников NVD NIST и GitHub Advisories.

Предоставление полной информации об уязвимостях, включая имеющиеся рекомендации по их устранению.

Отслеживание новых уязвимостей и изменения лицензионных соглашений в контролируемых программных проектах.

Реализация собственных политик применения открытых программных компонентов.

Интеграции в жизненный цикл разработки программного обеспечения (SDLC).

CodeScoring работает с наиболее распространенными репозиториями кода: GitHub, GitLab, BitBucket и Azure DevOps. Для полноценной работы в CI/CD пайплайне реализованы API и возможность интеграции через консольного агента.



(<https://zen.yandex.ru/id/5a95363da936f43fa2d8ea19>)

Подписывайтесь на канал "Anti-Malware" (<https://zen.yandex.ru/id/5a95363da936f43fa2d8ea19>) в Яндекс Дзен, чтобы первыми узнавать о новостях и наших эксклюзивных материалах по информационной безопасности.



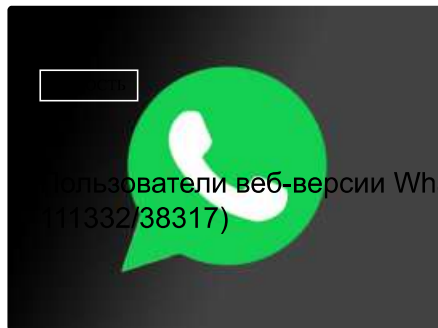
Makves скидывает 30% при миграции на отечественное DCAP-реше... (/news/2022-03-04-111332/38282)

(/news/2022-03-04-111332/38282)



(/news/2022-02-18-111332/38203)

нашли ещё одну критическую RCE-бр... (/news/2022-02-18-



(/news/2022-03-11-111332/38317)

пользователи веб-версии WhatsApp теперь могут проверить подл... (/news/2022-03-11-111332/38317)



 (/news/feed)

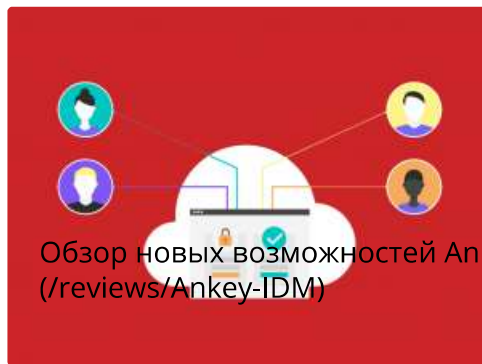
Главные новости



(/news/2022-03-24-111332/38397)

- 1 ФСТЭК России приостановила действие 56 сертификатов (Microsoft, Cisco, др.) (/news/2022-03-24-111332/38397)
- 2 Китайский бэкдор Gimmick портирован на macOS (/news/2022-03-23-114534/38391)
- 3 Эксперты составили топ-10 самых быстрых шифровальщиков (/news/2022-03-24-111332/38393)

ОБЗОР НЕДЕЛИ



Обзор новых возможностей Ankey IDM, средства управления учётными записями
(/reviews/Ankey-IDM)

(/reviews/Ankey-IDM)

Подпишитесь на новости

Ежедневная рассылка

Лучшие новости на день в вашем почтовом ящике

Еженедельная подборка

Дайджест популярных статей за неделю

Подписаться



(/interviews/2022-03-18/38358)

Вячеслав Кузьмин:

«Для Экспобанка острой стала проблема разграничения прав доступа» (/interviews/2022-03-18/38358)

КАТАЛОГ СЗИ

Средства защиты (/security)
Угрозы (/threats/information-security-threats)
Сертифицированные СЗИ (/certified/information_security_russia)
Реестр Anti-Malware.ru (/certified)

УСЛУГИ

Реклама (/advertisement)
Сертификация (/services/certification)
Индивидуальные тесты (/services/tests)

О НАС

Редакция (/team)
Контакты (/contact)
Авторы (/best-authors)
Прислать материал (/send_article)
Политика конфиденциальности (/privacy-policy)

Свидетельство о регистрации СМИ ЭЛ № ФС 77 - 68398, выдано федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) 27.01.2017

Разрешается частичное использование материалов на других сайтах при наличии ссылки на источник. Использование материалов сайта с полной копией оригинала допускается только с письменного разрешения администрации.

© ООО "АМ Медиа", 2005-2021. Все права защищены. (/terms_of_use)

(<https://attendee.gotowebinar.com/register/5394704745072711695?source=ammedia>)



On April 7, a new Russian software of the DCAP class is released. Orlan is an IB with a Russian soul. Register >>

(<https://orlansec.ru/>)

[Home \(/\)](#) » [News \(/news\)](#)



The next level of DevSecOps

On April 7, at an online meetup, Positive Technologies experts will tell you how to reach a new level of secure development using PT Application Inspector 4.0.

(https://promo.ptsecurity.com/application-inspector?utm_source=antimalware&utm_medium=banner-200-160&utm_campaign=ai4)

More » (https://promo.ptsecurity.com/application-inspector?utm_source=antimalware&utm_medium=banner-200-160&utm_campaign=ai4)

Google accuses two Russians of creating a powerful Glupteba botnet

Ekaterina Bystrova (/Users/Ekaterina-Bystrova) 08 december 2021 - 09:17

[Corporations \(/corporate_security\)](#)

[State \(/state_security\)](#)

[Windows \(/os/windows\)](#)

[Google \(/companies/google\)](#)

[Botnet \(/threats/botnet\)](#)



Google (/companies/google) accuses two Russian citizens of organizing a complex cyber operation and creating a botnet. According to the American Internet giant, the defendants infected more than a million Windows devices worldwide.

Dmitry Starovikov and Alexander Filippov - these are the names that appear in the appeal of Google. The corporation claims that Russian citizens were behind the Glupteba botnet attacks. Also mentioned are many Gmail and Google Workspace accounts that helped Filippov and Starovikov carry out cyberattacks.

The bot network, according to Google, was used for criminal purposes: to steal and unauthorized access to the credentials of users of Google accounts. Since 2020, cybercriminals have managed to infect over a million computers running Windows.

Glupteba's cyber campaign has gained momentum to such an extent that every day the attackers managed to replenish the ranks of bots with thousands of new devices. As a rule, criminals managed to infect devices using malicious sites, luring victims to them. Typically, such resources offered to download some software for free.

"At any moment, the entire power of the Glupteba botnet could be directed to organizing a powerful DDoS attack. It is also worth noting that Glupteba differs from other botnets in its complex technical implementation - for example, the use of blockchain technology," writes (https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/1_Complaint.pdf) (PDF) Google in its appeal to the Federal District Court for the Southern District of New York.

According to the American corporation, Glupteba operators attacked targets in the United States, India, Brazil, Vietnam and Southeast Asia.

NEXT MAIN NEWS »



(<https://zen.yandex.ru/id/5a95363da936f43fa2d8ea19>)

Subscribe to the "Anti-Malware" channel (<https://zen.yandex.ru/id/5a95363da936f43fa2d8ea19>) in Yandex Zen to be the first to know about news and our exclusive information security materials.

Read also

Against the backdrop of sanctions, Informzaschita launched an express audit of information security risks (/news/2022-03-21-111332/38372)

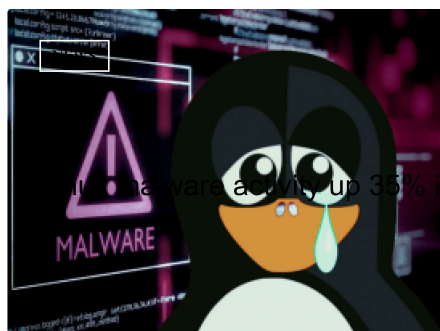
FSTEC of Russia suspended 56 certificates (Microsoft, Cisco, etc.) (/news/2022-03-24-111332/38397)

Vulnerabilities in Dell BIOS are relevant for millions of XPS, Inspiron, Vostro (/news/2022-03-22-114534/38382)



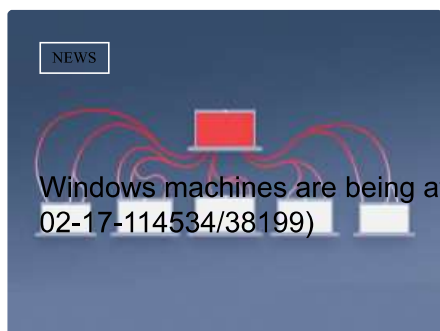
(/news/2022-02-22-111332/38223)

Kaspersky reported a record number of DDoS attacks in the history of... (/news/2022-02-22-111332/38223)



(/news/2022-01-17-1447/37970)

Anti-malware activity up 35% in 2021 (/news/2022-01-17-1447/37970)



(/news/2022-02-17-114534/38199)

Windows machines are being attacked by Kraken, a new Golang bot under development... (/news/2022-02-17-114534/38199)

[ANALYTICS \(/ANALYTICS\)](#)

An Overview of Secure Platforms and Overhead Big Data Security (/analytics/Market_Analysis/Big-Data-Protection)



(/analytics/Market_Analysis/Big-Data-Protection)

How to conveniently and profitably apply biometric authentication in a corporate environment (/analytics/Technology_Analysis/Corporate-Biometric-Authentication)



(/analytics/Technology_Analysis/Corporate-Biometric-Authentication)

Система анализа софта CodeScoring добавлена в реестр российского ПО (/news/2022-03-25-111332/38409)

Екатерина Быстрова (/Users/Ekaterina-Bystrova) 25 марта 2022 - 20:10

Малый и средний бизнес (/smb_security) Корпорации (/corporate_security)

Системы для анализа защищенности информационных систем (/security/security-check)

Аудит информационной безопасности (/security/Information-Security-Audit) Сканеры исходного кода (/security/source-code-analysis)



(/news/2022-03-25-111332/38409)

Система композиционного анализа программного обеспечения CodeScoring официально добавлено в реестр российского ПО. Официальный дистрибьютор продукта в России — компания Web Control.

Современная разработка ИТ-продуктов активно применяет программные компоненты с открытым исходным кодом (OSS, Open Source Software). Практически всегда таких компонентов на порядок больше, чем проприетарных.

Использование OSS даёт значимое ускорение разработки, но при этом его бесконтрольное использование увеличивает риски для безопасности. Для управления этими рисками применяются решения класса композиционного анализа ПО (SCA, Software Composition Analysis), которые автоматически определяют используемые OSS зависимости, показывают найденные в них уязвимости и предоставляют информацию об их устранении.

Продукт CodeScoring (<https://codescoring.ru/>) может повысить безопасность использования Open Source на всех этапах обеспечения жизненного цикла разработки программного обеспечения. База знаний CodeScoring содержит собираемый из крупнейших репозиторий реестр компонентов, который регулярно обогащается данными об имеющихся в них уязвимостях и лицензиях, получаемых из различных источников. CodeScoring поддерживает ключевые OSS экосистемы популярных языков программирования, такие как Maven, PyPi, NPM, RubyGems и др.

CodeScoring содержит следующие функциональные возможности:

Автообнаружение зависимостей — анализ состава кода, автоматическое нахождение файлов манифестов пакетных менеджеров, выявление прямых и транзитивных зависимостей открытого программного обеспечения (OSS).

Ведение реестра компонентов программных проектов (SBOM).

Проверка совместимости Open Source лицензий — выявление лицензий для обнаруженных OSS зависимостей и проверка их совместимости между собой на основании интегрированных политик.

Выявление уязвимых Open Source компонентов в программных проектах на основании актуальной информации из авторитетных источников NVD NIST и GitHub Advisories.

Предоставление полной информации об уязвимостях, включая имеющиеся рекомендации по их устранению.

Отслеживание новых уязвимостей и изменения лицензионных соглашений в контролируемых программных проектах.

Реализация собственных политик применения открытых программных компонентов.

Интеграции в жизненный цикл разработки программного обеспечения (SDLC).

CodeScoring works with the most common code repositories: GitHub, GitLab, BitBucket, and Azure DevOps. For full-fledged work in the CI / CD pipeline, APIs and the ability to integrate through the console agent are implemented.



(<https://zen.yandex.ru/id/5a95363da936f43fa2d8ea19>)

Subscribe to the "Anti-Malware" channel (<https://zen.yandex.ru/id/5a95363da936f43fa2d8ea19>) in Yandex Zen to be the first to know about news and our exclusive information security materials.



Makves discounts 30% when migrating to a domestic DCAP solution... (/news/2022-03-04-111332/38282)

(/news/2022-03-04-111332/38282)



found another critical RCE-bracket... (/news/2022-02-18-111332/38203)

(/news/2022-02-18-111332/38203)

NEWS

App web users can now check fake... (/news/2022-03-11-111332/38317)



(/news/2022-03-11-111332/38317)



 (/news/feed)

Top news



(/news/2022-03-24-111332/38397)

- 1 FSTEC of Russia suspended 56 certificates (Microsoft, Cisco, etc.) (/news/2022-03-24-111332/38397)
- 2 Chinese backdoor Gimmick ported to macOS (/news/2022-03-23-114534/38391)
- 3 Experts have compiled the top 10 fastest ransomware (/news/2022-03-24-111332/38393)



Ankey IDM New Features Overview, Account Management Tools (/reviews/Ankey-IDM)

(/reviews/Ankey-IDM)

Subscribe to news

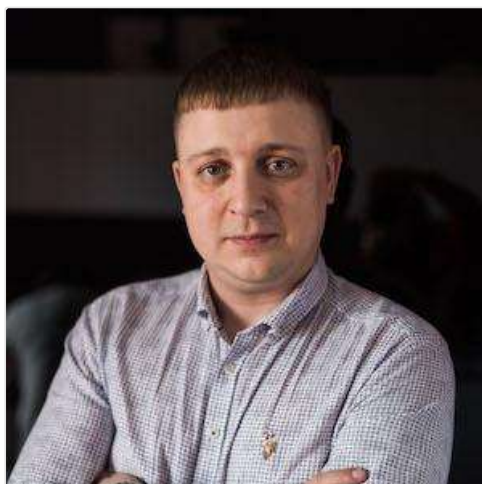
Daily Newsletter

The best news of the day in your inbox

Weekly compilation

Digest of popular articles for the week

Subscribe



(/interviews/2022-03-18/38358)

Vyacheslav Kuzmin:

"The problem of access rights differentiation has become acute for Expobank" (/interviews/2022-03-18/38358)

GIS CATALOG

Means of protection (/security)

Threats (/threats/information-security-threats)

Certified GIS (/certified/information_security_russia)

Registry Anti-Malware.ru (/certified)

SERVICES

Advertising (/advertisement)

Certification (/services/certification)

Individual tests (/services/tests)

ABOUT US

Editorial (/team)

Contacts (/contact)

The authors (/best-authors)

Send material (/send_article)

Privacy Policy (/privacy-policy)

Свидетельство о регистрации СМИ ЭЛ № ФС 77 - 68398, выдано федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) 27.01.2017

Разрешается частичное использование материалов на других сайтах при наличии ссылки на источник. Использование материалов сайта с полной копией оригинала допускается только с письменного разрешения администрации.

© ООО "АМ Медиа", 2005-2021. Все права защищены. (/terms_of_use)